안전한 전자 입찰 시스템에 관한 연구

박희운[†] · 이임영[††]

요 약

정보화 사회를 거치면서 네트워크의 발전과 관련해 많은 응용 분야들이 연구되고 있다. 이러한 응용 분야 중 전자 입찰은 그 중 한 예가 될 수 있을 것이다. 본 연구에서는 기존의 입찰 시스템을 전자화 하여 인터넷에서 사용하는데 그 초점을 맞춘다.

전자 입찰 시스템은 기존의 입찰 과정에서 발생되어 온 시간 및 비용의 비효율성을 극복할 수 있는 장점이 있다. 그러나 기존의 입찰 시스템을 전자화 하는 과정에서 안전성 및 공정성 부분에서 문제가 발생할 수 있다. 따라서 본 논문에서는 전자 입찰 서비스에 위협이 될 수 있는 문제점들 및 요구 사항을 살펴보고 기존의 방식이 이들 요구사항에 대해 어떻게 대처하는지 고찰할 것이다. 또한 제시된 모든 요구 사항을 만족하는 보다 안전하고 효율적인 새로운 전자 입찰 방식을 제안한다.

A Study on Secure Electronic Bidding System

Hee-Un Park[†] and Im-Yeong Lee[††]

ABSTRACT

In our modern information society, many subjects related to computer networks are studied. The electronic bidding system based on cryptology is one of such subjects. In this study, we focus upon the bidding system used in the internet electronically.

The electronic bidding system compared to the older version is time consuming and cost efficient in the process of bidding. However, there are many issues, that connected with the safety and the equality, to be resolved before the system can be applied in practice. Therefore, in this paper, we consider with the problems and requirements of the electronic bidding system and analyze the conventional electronic bidding systems based on the requirements. Also we propose the new secure efficient electronic bidding system that satisfies all requirements.

1. 서 론

네트워크의 급속한 발전과 더불어 컴퓨터의 보급 확산을 통해 현대 사회를 일컬어 “정보화 사회”라 하고 있다. 관공서 및 각 기업체에서는 기본적 업무 및 각종 문서 처리를 컴퓨터와 인터넷 및 E-mail을 통해 신속하게 수행하고 있다. 일상 생활에 있어서도 인터넷과 관련된 많은 서비스들이 연구되거나 제공되고 있는 실정이다. 그 대표적인 예를 살펴보면 전자 상거래, 전자 투표, 안전한 e-mail, 인터넷 통신 판매, 전자 입찰 등등이 있다.

본 연구에서는 이러한 인터넷 응용 분야 중, 기존의 입찰 과정을 전자화 하여 인터넷에서 사용하는데 그 초점을 맞춘다. 현행 입찰 방식은 그 용도와 성격에 따라 매우 다양하게 적용되고 있다. 복합 건물 건축 입찰, 상가 분양 및 입점, 미술품이나 일반 물건 입찰 등이 그 좋은 예가 될 것이다. 물론 그 외에도 다양한 종류의 입찰 방식이 있겠지만 인터넷의 성격상 입찰 공고자, 서버 그리고 입찰자 등의 요소들로 구성되는 전자 입찰 방식에 대해 고려하고자 한다. 이 방식은 입찰 공고시 공고자의 요구 사항이나 내정가 등이 인터넷을 통해 기재되고, 이에 대해 각 입찰

[†] 준회원, 순천향대학교 전산학과 박사과정
[††] 정회원, 순천향대학교 정보기술공학부 부교수

자가 시방서를 작성하여 최적의 가격 또는 최고 · 저의 가격이 산출되었을 때 자동적으로 입찰이 수행되는 방식이다.

전자 입찰 시스템은 기존의 입찰 과정에서 발생되어 온 시간 및 비용의 비효율성을 극복할 수 있는 장점이 있다. 그러나 전자 입찰의 경우 기존 방식을 전자화 하는 과정에서 제 3자에 의한 도청을 통해 시방서 및 개인 신원이 노출될 수도 있으며, 각 구성 요소간의 공모를 통해 안전성 및 공정성 부분에서 문제가 발생할 수 있다. 따라서 본 연구에서는 전자 입찰 서비스에 위협이 될 수 있는 문제점들 및 요구 사항을 지적하고, 기존의 방식이 어떻게 대처하는지 고찰할 것이다. 또한 안전성과 공정성 확보를 위해 필수적인 보안 요소를 적용함으로서 보다 안전하고 효율적인 전자 입찰 방식을 제안한다.

2. 전자 입찰 방식 고찰

본 장에서는 기존의 입찰 시스템을 전자화 하는데 있어 문제점 및 필요한 요소들이 무엇이 있는지 살펴보고, 기존의 방식이 이에 대해 어떻게 대처하는지 확인한다.

2.1 전자 입찰 시스템의 문제점

기존의 입찰 시스템을 전자화하는 과정에서 입찰자, 입찰 공고자, 서버 등의 참여 요소들이 필요하게 된다. 이러한 과정에서 많은 사안들이 고려되어야 하며, 일반적으로 네트워크 상에서의 안전한 정보 전송 및 저장이 관건이 된다. 또한 각 요소간의 공모를 막기위해 서버는 입찰 공고자에게 있어 독립성을 가지고 있어야 한다. 이는 입찰에 있어 기본적인 요구 사항이며, 신뢰성을 확보하는데 중요한 사안이다. 다음은 전자 입찰 수행시 발생될 수 있는 문제점을 제시한 것이다.

(1) 네트워크 상의 메시지 유출

전자 입찰시 입찰자 및 입찰 공고자의 정보는 공개 네트워크를 통해 서버에게 전송 및 수신되게 된다. 이때 부정한 제 3자 또는 도청자에 의해 정보가 그대로 유출된다면 입찰의 공정성이 무너질 수 있게 된다. 이를 막기위해서 네트워크를 통해 전송 및 수신되는 정보는 암호 기법과 같은 안전한 도구를 이용해 불법적인 제 3자로부터 보호되어야 한다.

(2) 입찰자와 서버 사이의 공모

이러한 종류의 공모는 서버가 입찰자들의 제시 가격들을 접수받은 다음, 특정 입찰자에게 그 정보를 제공함으로서 입찰 시 부정을 저지르게 된다. 이를 방지하기 위해 서버는 입찰자들의 입찰가를 미리 알 수 없어야 하고, 입찰자들의 개인 정보는 보호되어야 한다.

(3) 입찰자간의 공모

이 상황은 입찰 공고자의 입찰 예정가를 미리 알 경우, 입찰자들이 입찰가에 대한 담합을 통해 공모가 발생하는 경우이다. 이를 방지하기 위해서는 누구나가 입찰에 참여할 수 있어야 하며, 입찰자의 신원이 보장되어야 한다. 또한, 유찰 제도를 도입함으로써 입찰 공고자의 피해를 막을 수 있어야 한다.

(4) 입찰자와 입찰 공고자간의 공모

이러한 부정은 입찰 공고자가 입찰자들에 대한 입찰 정보를 보유하고 있는 상황에서, 특정 입찰자에게 입찰 예정가와 상대방 입찰자의 입찰 정보를 유출함으로서 일어날 수 있다. 이를 방지하기 위해서는 입찰 공고자와 서버는 독립성을 유지해야 하며, 입찰자들의 정보는 보호되어야 한다.

또 다른 위험 요소는, 특정 입찰자를 제외한 상태에서 나머지 입찰자의 입찰가를 변조 및 누락시킬 가능성이 있다. 이를 방지하기 위해서는 입찰 이후, 누구나 납득이 가능하도록 정확하게 모든 정보는 공개되어야 한다.

(5) 서버의 독단

이 사안은 서버가 특정 입찰자를 위해 나머지 입찰자의 정보 또는 입찰 공고자의 입찰 정보를 누락 및 변조할 가능성을 지적한 것이다. 이를 위해서는 입찰 참여시 입찰 정보의 정확한 등록 여부 확인이 가능해야 하며, 입찰이 끝난 다음 집행의 공정성을 위해 모든 정보는 공개되어야 한다.

2.2 전자 입찰 시스템의 요구 사항

전자 입찰 시스템은 위의 다섯 가지 문제점을 모두 극복할 수 있어야 하며, 이들 중 하나라도 해결이

안될 경우에는 그 안전성을 보장할 수 없을 것이다. 따라서, 전자 입찰 시스템은 다음과 같은 요구 조건을 만족해야 한다.

(1) 독립성

전자 입찰 시스템의 각 요소들은 자신들의 독자적인 자율성을 보장하기 위해 독립성을 확보해야 한다.

(2) 비밀성

공개 네트워크 상에서 각 구성 요소간의 개별 정보는 어느 누구에게도 노출되어서는 안된다.

(3) 무결성

입찰 수행 시 입찰자 자신의 정보를 확인 가능하게 함으로서 누락 및 변조 여부를 확인할 수 있어야 한다.

(4) 공평성

입찰이 수행될 시 모든 사람들이 이해할 수 있도록 모든 정보는 공개되어야 한다.

(5) 안전성

각 입찰 참여 요소간의 공모는 방지되어야 하며, 입찰 공고자 및 서버의 독단이 발생되어서는 안된다.

2.3 기존 방식 고찰

(1) 인터넷 온라인 입찰 시스템

본 절에서 소개하는 방식은 인터넷과 같은 온라인 상에서 입찰이 가능하도록 구성된 방식으로(이하 LKR 방식이라 함) 내용은 다음과 같다[6].

▶ 시스템 계수

본 방식에서 사용되는 시스템 계수는 다음과 같다.

- M : 입찰 내용
- KS_c : 입찰자의 관용키
- KR_c, KR_s : 입찰자의 서명키와 확인 키
- KU_s, KU_c : 서버의 공개키와 복호화 키
- H : 일방향 해쉬 함수[11]

▶ 프로토콜 분석

1) 등록 : 입찰자는 자신의 서명 확인키 KR_s를 서버에게 제출하며, 서버는 각 입찰자들에게 독립적 ID를 생성해 서명을 붙여 전송한다.

: $KU_c(ID)$

2) 입찰

2.1) 입찰 공고 : 서버는 S/MIME와 같은 안전한 메일을 이용해 입찰 발생을 공고한다.

2.2) 입찰 : 입찰자는 입찰 내용에 해쉬를 취해 서명을 수행한 다음 관용키로 암호화하여 서버에게 전송한다.

: $KS_c(KR_c(ID||M||H(M)))$

2.3) 입찰 접수 확인 : 서버는 입찰자로부터 전송된 입찰 정보를 다음의 형태로 공개 보드에 등록한다.

: $KS_c(KR_c(ID||M||H(M)))$

3) 낙찰자 공개 : 입찰자는 자신의 관용키를 서버에 제공하며, 서버는 이를 공개함으로서 모두가 확인할 수 있도록 한다.

: $KR_s(K'S_c(KS_c(KR_c(ID||M||H(M)))))$

$= ID||M||H(M)$

▶ LKR 방식 분석

본 방식은 S/MIME과 같은 안전한 전송로를 구축함으로서 제 3자의 도청 및 변조를 방지하고, 입찰 내용에 해쉬를 취하여 입찰자의 서명을 붙임으로서 무결성 및 부인 봉쇄를 가능하게 하는 방식이다.

그러나 이 방식은 등록 절차시 각 입찰자의 서명 확인키가 노출되며 ID가 입찰 공고자의 서명만을 수행한 상태에서 전송되므로, 입찰자의 신원 노출에 따른 입찰 정보 유출이 발생될 가능성이 있다. 동시에 입찰 공고자와 서버가 하나로 구성되어 있기 때문에

그림 1. LKR 방식 흐름도

특정 입찰자와 사전 공모를 할 경우 입찰자들의 입찰 정보를 제공함으로서 부정이 가능해 진다. 또한, 이 방식은 입찰 공고자의 시방서(First Copy Registration)가 공개되지 않는다. 그러므로 프로토콜처럼 입찰자의 관용키를 제공받은 다음 입찰 예정가를 공개 보드에 등록할 경우, 서버가 임의로 입찰 예정가를 변경 조작하더라도 진위를 확인할 수 없으며, 유찰의 근거가 마련되지 않는 문제가 발생한다.

따라서 본 방식은 공평성은 확보하고 있으나 독립성, 비밀성 및 안전성에 문제를 안고 있다 하겠다.

(2) 안전한 전자 입찰 시스템

이 방식은 온라인 상에서 각 구성 요소간의 결탁을 방지할 목적으로 제안된 방식이다(이하 PL 방식이라 함)[7]. 이 방식에서는 입찰자와 서버간에 발생 가능한 공모를 그룹 서명 방식[5]을 이용하여 방지하였고, 입찰 공고자가 하나 이상의 입찰 예정가를 선택하여 이들 중 하나를 서버가 랜덤하게 선택하게 함으로서 입찰자와 입찰 공고자 사이의 결탁을 방지하고 있다. 동시에 입찰 이후 입찰 정보를 공개 보드 상에 공개하게 함으로서, 서버나 입찰 공고자의 독단을 방지하고 있다.

▶ 시스템 계수

다음 방식에서 사용되는 시스템 계수는 다음과 같다.

- I_j : 입찰자
- ID_j : 입찰자의 식별자 ($j = 1,...,k$)
- $\$_j$: 입찰자의 입찰가
- S : 서버
- K : 입찰 공고자
- $\$K_t$: 입찰 공고자의 입찰 예상가 (단, $t = \{1,...,l\}$)
- K_p, K_s : 입찰 공고자의 공개키와 비밀키
- S_p, S_s : 서버의 공개키와 비밀키
- $I_{j1}...I_{jk}$, I_n : 입찰자의 그룹 서명키와 확인키 (단 j는 입찰자들의 수, $n = j*m$)

▶ 프로토콜 분석

· 준비 단계

1) 입찰 공고자는 입찰 공고를 인터넷상에 낸 다음, 입찰자를 모집한다.

: 이때 입찰자는 자신의 식별자 ID_j를 입찰 공고자에게 제공한다.

2) 입찰 공고자는 그룹 서명키 $I_{j1}...I_{jk}$을 입찰자 j에게 제공한 다음, 확인키 I_n을 서버에게 제공한다.

3) 입찰 공고자는 다음과 같이 입찰 예상가들을 자신의 공개키로 암호화하여 서버에게 제공한다.

: $K_p(\$K_1),...K_p(\$K_n)$

4) 서버는 입찰 공고자로부터 수신된 입찰 예상 정보들 중 랜덤하게 하나를 선택하여 저장하고, 이를 자신의 암호화키로 암호화하여 입찰 공고자에게 전송한다. 이를 통해 입찰 공고자의 독단 및 입찰자와의 공모를 막도록 하고 있다.

: $S_p(K_p(\$K_t))$

· 실행 단계

5) 입찰자는 자신의 ID_j와 입찰가 $\$_j$를 입찰 공고자의 공개키로 암호화한 다음 그룹 서명키를 이용해 서명한다. 이를 서버에게 전송함으로서 제 3자에 의한 정보 도청을 막을 수 있다.

: $I_{ji}(K_p(ID_j || \$_j))$ (단, $i = \{1,...,k\}$)

6) 서버는 입찰자로부터 수신된 메시지를 그룹 서명 확인키를 통해 다음과 같이 입찰자들이 정당함을 확인한다. 그런 다음 이를 입찰 공고자에게 전송한다.

: $I_n(I_{ji}(K_p(ID_j || \$_j))) = K_p(ID_j || \$_j)$

7) 입찰 공고자는 서버로부터 수신된 입찰 정보를 자신의 비밀키를 이용하여 확인한다.

: $K_s(K_p(ID_j || \$_j)) = ID_j || \$_j$

· 공개 단계

8) 입찰 공고자는 입찰자들의 식별자와 입찰가를 공개 보드에 공개한다.

9) 입찰 공고자는 서버의 도움을 얻어 입찰 예정가를 공개 보드에 공개한다.

: $S_s(S_p(K_p(\$K_t))) = (K_p(\$K_t))$

: $K_s(K_p(\$K_t)) = \$K_t$

10) 입찰 예정가에 가장 근사한 입찰자가 자동으로 입찰된다.

▶ PL 방식 분석

이 방식은 입찰 공고자와 서버가 공모할 경우, 입찰 예정가 및 입찰가 조작이 가능한 문제점을 가지고 있다. 또한 입찰 공고자가 시방서(First copy registration)작성시 서버가 랜덤하게 선택하게 함으로서 최적의 효율성을 확보하지 못하는 문제점을 가지고 있다.

그림 2. PL 방식 흐름도

3. 새로운 방식 제안

본 논문에서는 제안하는 방식은 기존의 PL 방식을 개선한 방식으로서, 각 입찰 참여 요소간의 공모를 방지하고 입찰자 신원을 보장하기 위해 그룹 서명 방식[5] 및 Secure Selection 기법[8]을 적용하고 있다. 또한 입찰 공고자가 시방서를 제출하여 적정 입찰가를 얻지 못할 경우 다시 유찰을 실시함으로서, 최적의 입찰 예정가를 얻도록 하고 있다. 동시에 모든 정보를 공개 보드 상에 공개하게 함으로서, 서버나 입찰 공고자의 독단을 방지할 수 있는 안전한 방식이라 할 수 있을 것이다.

3.1 시스템 계수

전자 입찰 시스템에서 사용되는 시스템 계수는 다음과 같다.

- I_i : 입찰자 (i = 1, 2, ..., n : 참여 입찰자 수)
- ID_i : 입찰자 I_i의 가명 식별자
- V_i : 입찰자 I_i의 제시 입찰가
- S : 서버
- A : 입찰 공고자
- AV : 입찰 공고자의 입찰 예상가
- S_{pi}, S_{si} : 입찰자의 공개키와 비밀키
- BS_{pi}, BS_{si} : 입찰자의 가명 공개키와 비밀키
- K_p, K_s : 입찰 공고자의 공개키와 비밀키
- A_p, A_s : 서버의 공개키와 비밀키
- $SI_{i1}...SI_{ik}$, DI_n : 입찰자의 그룹 서명키와 확인키 (n = i*k)

3.2 전자 입찰 프로토콜

(1) 입찰 공고 및 사전 준비 단계

1) 입찰 공고자는 서버의 공개 보드 상에 입찰 공고를 낸 다음, 입찰자를 모집한다.

2) 서버는 모집된 입찰자들이 자유로이 가명 식별자를 선택하도록 한다. 이때 입찰자들 간에 독립성을 유지하고, 자유롭고 정당한 입찰을 위해 입찰자는 ID_i 및 자신의 비밀키에 대해 자신의 공개키로 암호화하여 서버의 공개 보드에 등록한다. 동시에 입찰자는 자신의 가명 식별자에 대한 공개키 및 비밀키를 생성해 공개키를 공개 보드에 등록한다.

: $S_{pi}(ID_i||S_{si}||Cert(S_{pi}))$, BS_{pi}

3) 입찰 공고자는 다음과 같이 입찰자들의 가명 공개키를 이용해 암호화하여 그룹 서명키를 입찰자에게 제공하고, 그룹 확인키를 서버의 공개키로 암호화한 $A_p(DI_n)$를 서버에게 전송한다.

: $BS_{pi}(SI_{i1}...SI_{ik})$

4) 입찰 공고자는 입찰 예상가를 자신의 공개키로 암호화하여 시방서를 작성한다. 그런 다음 자신의 인증서를 첨부해 서버에게 전송한다. 이렇게 암호화를 수행함으로서 서버의 독단을 막을 수 있게된다.

: $K_p(AV)||Cert(K_p)$

5) 서버는 공고자로부터 수신된 정보를 확인한 다음 이를 서버용 디렉토리에 저장하고, 자신의 서명을 수행해 공개한다. 이를 통해 정당한 입찰 공고자의 시방서를 수신했음을 확인시키게 되며, 입찰 공고자와 서버간의 입찰가 변조 공모를 막을 수 있게 된다.

: $A_s(K_p(AV)||Cert(K_p))$

(2) 입찰 수행 단계

6) 입찰자는 자신의 가명 ID_i와 입찰가 V_i를 공고자의 공개키로 암호화한 다음 그룹 서명키를 이용해 수신자 지정 그룹 서명을 수행한다. 이를 서버 및 입찰 공고자에게 전송함으로서 제 3자에 의한 정보 도청을 막을 뿐만 아니라 입찰 공고자 및 서버의 변조 및 독단을 막을 수 있다.

: $SI_{ik}(K_p(ID_i||V_i))$

7) 서버는 그룹 서명 확인키를 통해 입찰자들이 정당함을 확인한 다음 이를 서버용 디렉토리에 저장하고, 공개 보드에 등록한다. 이를 통해 입찰자는 자신의 입찰가가 정확하게 등록되었음을 확인한다.

: $DI_n(SI_{ik}(K_p(ID_i||V_i))) = K_p(ID_i||V_i)$

(3) 공개 및 낙찰단계

8) 입찰 공고자는 자신의 비밀키를 이용하여 공개 보드 상에 암호화된 입찰 예정가를 공개한다. 입찰자의 입찰 정보를 미리 공개하지 않는 이유는 입찰 공고자와 서버간의 공모를 통해 입찰가 조작을 방지하기 위해서이다.

: $K_s(K_p(AV))||Cert(K_p) = AV||Cert(K_p)$

9) 입찰 공고자는 자신의 비밀키를 이용하여 입찰자들의 입찰 정보를 공개 보드에 공개한다.

: $K_s(K_p(ID_i||V_i)) = ID_i||V_i$

10) 시방서 조건에 대해 최적의 가명 ID_i가 자동으로 채택된다. 만약 조건이 맞지 않을 경우 유찰을 통해 다시 입찰 단계를 수행하게 된다.

11) 가명 ID_i에 실 입찰자는 자신의 비밀키를 이용하여 암호화된 개인 정보를 복호화함으로서 낙찰된다.

: $S_{si}(S_{pi}(ID_i||S_{si}||Cert(S_{pi}))) = ID_i||S_{si}||Cert(S_{pi})$

그림 3. 제안 방식 흐름도

3.3 제안 방식 분석

본 고에서 제안한 방식은 다음과 같은 특징을 통해 상기 요구 사항 및 효율성을 확보하고 있다.

(1) 독립성 확보

각 입찰자는 가명 ID를 사용함으로서 자신의 신원을 보장하고 누구나가 입찰에 참여 가능하다. 또한 입찰 정보 및 공고자의 시방서 정보는 공개키로 암호화되어 서버에게 전송되고, 서버는 이를 자신의 디렉토리 및 공개 디렉토리에 저장한다. 이러한 일련의 과정을 통해 각 입찰 요소간의 독립성을 확보하게 되며, 공모 및 독단과 같은 부정에 대해 공정성을 확보하게 된다.

(2) 비밀성 확보

입찰자들의 입찰 정보는 수신자 지정 그룹 서명 방식을 통해 전송되므로, 공개 네트워크 상에서 발생되는 어떠한 부정한 행위에 대해서도 정보 확인이 불가능하다. 또한 입찰 공고자의 시방서 내용 역시 공개키 암호화 방법을 이용하여 공개 디렉토리에 저장됨으로서 비밀성을 보장하고 있다. 이러한 특성은 네트워크 상에서의 메시지 유출을 방지하고, 입찰자와 서버 사이의 공모, 입찰자간의 공모 및 입찰자와 입찰 공고자간의 공모를 막는데 매우 유용하게 사용된다.

(3) 무결성 확보

입찰자들이 서버에게 전송한 입찰 정보는 공개 디렉토리에 저장되고 동시에 서버의 디렉토리에 저장된다. 입찰자들은 공개된 입찰 정보를 통해 자신의 입찰 정보의 정당성을 확인함으로서 무결성을 확보하고 있다. 이러한 특성은 입찰 공고자 및 서버로부터 중간 단계에서의 입찰가 확인이 불가능하게 하므로, 입찰자와 서버 사이의 공모, 입찰자와 입찰 공고자간의 공모 및 서버의 독단을 막는데 사용된다.

(4) 공평성 확보

공개 디렉토리에 암호화되어 저장되어진 입찰 정보 및 시방서 정보는 입찰 확인 과정에서 모두에게 공개된다. 이때 공모 및 독단에 따른 문제가 발생할 경우 각 참여 요소들의 확인이 가능하므로 공평성을 획득하고 있다.

(5) 안전성 확보

제안 방식은 상기 네 가지 특성들을 모두 만족함으로서, 각 단계별로 발생 가능한 각 입찰 참여 요소간의 공모를 방지하고 있으며, 입찰 공고자 및 서버의 독단을 예방하고 있다. 이와 같이 안전성을 확보함으로서 입찰 당사자간의 신뢰성을 제공하고 있다.

(6) 효율성 확보

본 방식은 기본 요구 사항을 모두 만족하면서, 원하는 최적의 입찰 예정가를 공시하게끔 구성하고 있

표 1. 각 방식별 비교 분석표

요소 \ 방식	LKR 방식	PL 방식	제안 방식
독립성	×	○	○
비밀성	△	○	○
무결성	△	○	○
공평성	○	○	○
안전성	×	△	○
효율성	△	△	○
구성 요소	서버, 입찰자	입찰 공고자, 서버, 입찰자	입찰 공고자, 서버, 입찰자
사용 방식	관용키 방식, 공개키 서명 방식,	공개키 방식, 그룹 서명 방식	공개키 방식, Secure Selection, 수신자 지정 그룹 서명 방식

○: Good, △: Normal, ×: Weak

으므로, PL 방식의 문제점을 해결하고 있다. 동시에 시방서에 대해 입찰가가 만족하지 않을 경우 유찰을 수행하도록 하고 있다.

다음은 각 방식별 특성들을 비교 분석한 결과이다.

4. 결 론

정보화 사회의 진전은 많은 인터넷 응용 분야를 창출하고 있다. 이들 분야 중 전자 입찰 시스템은 좋은 일례가 될 것이다. 본 연구에서는 인터넷을 통하여 제시된 입찰 조건 및 내용을 기초로 최적 또는 최대·저 가격을 제시한 입찰자의 시방서를 자동적으로 낙찰시키는 시스템을 고려해 보았다. 이를 기초로 기존의 일반적인 입찰 방식을 전자 입찰 시스템으로 도입하는 과정에서 발생 가능한 문제점들이 무엇인지 살펴보았으며, 전자 입찰 시스템을 구성함에 있어 어떠한 요구 사항이 필요한지 고찰하였다.

기존의 LKR 방식은 서버를 통해 입찰 공고자의 역할을 동시에 수행하게 함으로서 서버의 독단이 발생될 우려가 있었으며, 입찰자와의 공모를 막을 방법이 없었다. 또한 입찰자의 ID 및 서명 확인키가 노출되기 때문에 신원 노출에 따른 입찰 정보 유출이 발생할 수 있었다. PL 방식은 그룹 서명을 이용하여 입찰자와 서버의 공모를 막게 하였으며, 입찰 공고자의 공개키로 암호화된 입찰 예정가를 서버의 암호화키로 암호화함으로서 입찰자와 입찰 공고자의 공모를 막을 수 있게 하였다. 그러나 이 방식에서는 입찰 공고자와 서버간의 공모가 이뤄질 경우 입찰 예정가 조작을 통해 부정을 일으킬 수 있고, 최적의 입찰 예정가 선택이 힘들다는 단점을 가지고 있다.

이에 대해 제안 방식은 Secure Selection 기법, 가명 ID 및 수신자 지정 그룹 서명 방식을 적용하여 모든 입찰 정보의 안전한 공개가 가능하고, 입찰자 신원을 보장하고 있다. 이를 통해 각 참여 요소간의 공모가 무의미하게 되고, 서버 및 입찰 공고자의 독단이 불가능하다는 장점을 갖는다. 또한 시방서 작성을 통해 입찰가가 맞지 않을 경우 유찰을 통해 최적의 입찰가를 받을 수 있도록 함으로서 효율성을 확보하는 방식이다.

정보화 사회에 있어 인터넷과 같은 공용 네트워크를 통한 정보 교류는 필수적이며, 이를 이용한 각종 서비스들 또한 매우 광범위하게 적용되리라 본다. 본 고에서 제안한 전자 입찰 시스템 역시 그 한 부분을 차지하리라 믿으며, 이를 통한 안전하고 공정한 전자 상거래 문화 정착에 기여하리라 판단된다.

참 고 문 헌

[1] A. Fiat and A. Shamir, "How to prove yourself: practical solutions to identification and signature problems, Advances of Cryptology", Proc. Of CRYPTO'86 Springer-Verlag, pp.186-194.

[2] William stallings, "Network and Internetwork Security", Prentice Hall International Edition, 1995.

[3] R. Rivest, A. Shamir and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM, v.21, n.2, Feb 1978, pp.120-126.

[4] R. Rivest, A. Shamir and L. Adleman, "Cryptographic communications System and method", U.S. Patent #4,405,829, 20 Sep 1983.

[5] D. Chaum, "Group Signatures", Advances in Cryptology-EUROCRYPT '91 Proceedings, Springer-Verlag, 1991, pp.257-265.

[6] 이종후, 김재명, 류재철, "인터넷 온라인 입찰 시스템 설계", 한국정보과학회 '98 봄 학술발표논문집, 1998, pp.258-260.

[7] 박희운, 이임영, "안전한 전자 입찰에 관한 연구", 한국정보처리학회 '98 가을 학술발표논문집, 1998.

[8] K. Viswanathan, C. Boyd and E. Dawson, "Secure Selection Protocols", ICISC '99 Pre-Proceedings, Springer-Verlag, 1999, pp.61-66.

[9] 박희운, 이임영, "안전한 수신자 지정 그룹 서명 방식에 대한 고찰," 한국멀티미디어학회 '99 추계학술발표논문집, 1999, pp.36-41.

[10] S. J. Kim, S. J. Park and D. H. Won, "Nominative Signatures", Proc. ICEIC'95, 1995, pp.II-68~II-71.

[11] R. Rivest, "The MD5 Message Digest Algorithm", RFC 1321, Apr 1992.

[12] C. Boyd, "Digital Multisignatures", Cryptography and Coding, H.J. Beker and F.C. Piper, eds, Oxford:Clarendon Press, 1989, pp.241-246.

박 희 운

1997년 순천향대학교 전산학과 졸업
1997년~1999년 순천향대학교 전산학과 대학원 졸업(공학석사)
1999년~현재 순천향대학교 전산학과 박사과정 재학중
관심 분야 : 암호이론, 컴퓨터 보안

이 임 영

1981년 홍익대학교 전자공학과 졸업
1986년 일본 오오사카대학 통신공학과(석사)
1989년 일본 오오사카대학 통신공학과(박사)
1989년~1994년 한국전자통신연구원 선임연구원
1994년~현재 순천향대학교 정보기술공학부 부교수
관심분야 : 암호이론, 정보이론, 컴퓨터 보안